REMARKS

The Examiner is thanked for the thorough examination of the present application. The Pre-Appeal Board is also thanked for properly withdrawing the prior rejections. The patentability of the claims is discussed below.

I. The Claimed Invention

The invention, as recited in independent Claim 1, for example, is directed to a cryptographic device that includes a cryptographic module and a communications module removably coupled thereto. The cryptographic module includes a first housing, a user Local Area Network (LAN) interface carried by the first housing, and a cryptographic processor carried by the first housing and coupled to the user LAN interface. The cryptographic module also includes a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing. Furthermore, the communications module includes a second housing and a network wireless LAN interface carried by the second housing coupled to the cryptographic processor and switchable between wireless LAN modes.

Independent Claim 11 is directed to a similar cryptographic device, and independent Claims 21 and 25 are directed to related methods. Independent Claim 29 is directed to a related communications system.

II. The Claims Are Patentable

The Examiner rejected independent Claims 1, 11, 21, 25, and 29 over Dhir et al. in view of Cheng in further view of newly cited Hamlin et al. Applicants submit that the newly cited Hamlin et al. reference is at best just cumulative of the Klein reference previously cited. Accordingly, even a selective combination of the prior art fails to disclose the cryptographic module including a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing.

Dhir et al. is directed to a programmable integrated circuit, namely a field programmable gate array (FPGA), that can be used to handle different wireless local area network (WLAN) communication specifications. The integrated circuit includes a transceiver coupled to programmable gates, memory coupled to the programmable gates for storing instructions for programming a first portion of the programmable gates with a selected one of a first type of a medium access layer and a second type of a medium access layer. The first type of the medium access layer is different from the second type of medium access layer, though both the first type of the medium access layer and the second type of the medium access layer are compatible with the transceiver. The memory is configured for storing instructions for programming a second portion of the programmable gates as a baseband controller. (See, e.g., Col. 2, lines 14-49, of Dhir et al.).

The Examiner correctly acknowledges that Dhir et al. fails to teach a cryptographic module and a communications module that are removably coupled to one another, and a cryptographic

module including a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing. The Examiner then turned to Cheng for one of these critical deficiencies. Cheng is directed to an add-on card for a computer that is detachable from the computer and allows the computer to communicate with both wired and wireless networks. The add-on card includes an access control circuit, volatile and non-volatile memory, a wireless transmission module, and a network connection module. The network connection module has both an antenna for communicating with a wireless network, and a standard network cable port for connecting to a wired network. (See, e.g., paragraphs 0009-0010 of Cheng).

The Examiner still further recognized that even a selective combination of Dhir et al. and Cheng fails to disclose the cryptographic module including a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing. The Examiner turned to Hamlin for this critical deficiency. Hamlin is directed to a device including encryption circuitry enabled by comparing an operating spectral signature to an initial spectral signature.

Applicants submit that the Examiner mischaracterized Hamlin, as it fails to disclose the cryptographic module including a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing. The Examiner contended that Col. 4, lines 5-8, of Hamlin, which are reproduced below for reference, somehow disclose the claimed cryptographic module including a tamper circuit for disabling the

cryptographic processor based upon tampering with the first housing:

> "Attempts to tamper with the device 2 which alter the measured spectral characteristic of the clock signal 20 will disable the encryption circuitry 4 and prevent chosen plaintext attacks."

Indeed, Hamlin merely discloses disabling encryption circuitry based upon an alteration of a measured spectral characteristic of a clock signal or other internal signal. The measured spectral "characteristic may be, for example, a DC component of a power signal 20, or the convolution of such signals." (See Hamlin, Col. 4, lines 11-14). Nowhere does Hamlin disclose or suggest the cryptographic module includes a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing.

Applicants further submit that a person having ordinary skill in the art would not recognize the recitations of "tampering or probing with the device" in the context of changing the spectral characteristic of a clock signal or a power signal, as teaching a tamper circuit for disabling the cryptographic processor based upon tampering with said first housing. Accordingly, Hamlin fails to disclose a tamper circuit for disabling the cryptographic processor based upon tampering with said first housing, as recited in the independent claims.

Applicants further submit that the Examiner's combination of Dhir et al., Cheng, and Hamlin is improper, as a person having ordinary skill in the art would not turn to Cheng to combine with Dhir et al. and Hamlin to arrive at the claimed

invention. More particularly, as an initial matter, Dhir et al. is directed to a programmable logic device for a WLAN. The communications module and the cryptographic module are purposely on a single circuit board (330), as illustrated in Fig. 8 of Dhir et al. Combining Dhir et al. with Cheng so that the communications module and the cryptographic module would be removably coupled would require splitting the communications and cryptographic modules from the single circuit board.

Moreover, using Cheng as a motivation to modify Dhir et al. would result in arbitrarily dividing the circuitry of Dhir et al. between the antenna 336 and the WLAN transceiver 301, the antenna being outside the circuit board and downstream from both the communications and cryptographic modules. This is because Cheng discloses removably coupling the communications modules to a connector portion, including a physical connector and antenna. Accordingly, even if there was some proper motivation to combine Dhir et al. and Cheng, the claimed invention is not produced because the removable coupling is not between the communications module and the cryptographic module.

Still further, one of ordinary skill in the art would not turn to the security device including a spectral signal comparison data security system to combine with the programmable integrated circuit from Dhir et al. and the add-on card for a computer that is detachable from the computer and allows the computer to communicate with both wired and wireless networks from Cheng. In other words, the Examiner is attempting to combine an FPGA for a wireless LAN with a PCMCIA network add-on card and a device including cryptosystem validation. Applicants

submit that the Examiner is merely combining disjoint pieces of the prior art in an attempt to arrive at the claimed invention, and that the Examiner's combination of references is improper.

Accordingly, it is submitted that independent Claims 1, 11, 21, 25, and 29 are patentable over the prior art. Their respective dependent claims, which recite yet further distinguishing features, are also patentable over the prior art and require no further discussion herein.

III. CONCLUSION

In view of the arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a Notice of Allowance is requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,

DAVID S. CARUS
Reg. No. 59,291
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330
Attorneys for Applicants